Vol. 3, No. 3, Desember 2022, hal. 283-290

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Akuisisi Bukti Digital Pada Aplikasi Michat di Smartphone Menggunakan Metode National Institute of Standards and Technology (NIST)

Soni[1], Regiolina Hayami[1], Muhammad hamadi[1*]
Email: soni@umri.ac.id, regiolinahayami@umri.ac.id2, 170401012@student.umri.ac.id

[1]Teknik Informatika, Ilmu Komputer, Universitas Muhammadiyah Riau

Diterima: 01 Desember 2022 | Direvisi: - | Disetujui: 19 Desember 2022

Abstrak

Perkembangan teknologi di dunia perangkat mobile semakin berkembang. Namun dari perkembangan tersebut memiliki dampak kerugian salah satunya adalah tindakan cybercrime. Cybercrime adalah tindak kejahatan yang menggunakan teknologi informasi, Salah satu penyalahgunaan teknologi smartphone yang termasuk kasus cybercrime yang cukup banyak ditemukan di Indonesia antara lain prostitusi online anak dibawah umur. Hal ini dilakukan dengan memanfaatkan media sosial yakni michat sebagai media komunikasinya. Fitur "chatting dengan pengguna terdekat" dengan mengunggah status yang dapat terkoneksi dengan area sekitar dalam radius jarak tertentu dan setelah terhubung pelaku dan calon pelanggannya akan saling bernegosiasi dan bertran saksi hingga akhirnya bertemu. Untuk menghilangkan bukti digital berupa percakapan transaksi dalam pesan, biasanya pelaku akan menghapus history dari pesan yang mengakibatkan hilangnya data yang dapat dijadikan barang bukti dan pelaku dapat terhindar dari jebakan hukum, yang pada akhirnya secara online. prostitusi akan semakin marak. Untuk menindaklanjuti kegiatan Prostitusi Online, perlu dilakukan mobile forensik untuk menemukan barang bukti yang kemudian berguna untuk diberikan kepada pihak berwajib. Penelitian ini menggunakan metode National Institute of Standards and Technology (NIST).

Kata kunci: *Kejahatan cyber, Michat, Mobile Forensik, prostitusi online, NIST*

Acquisition of Digital Evidence on the MiChat Application on Smartphones Using the National Institute of Standards and Technology (NIST) Method

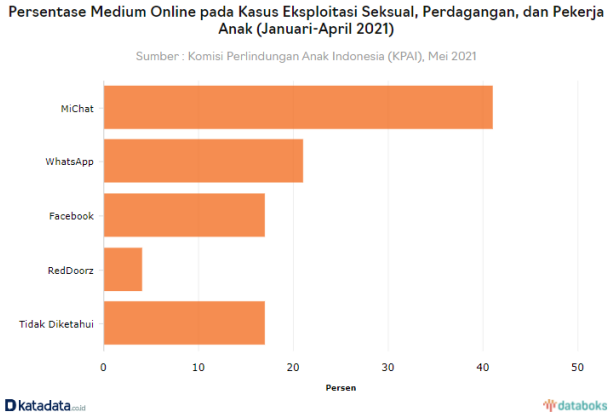
Abstract

The development of technology in the world of mobile devices is growing. However, these developments have a detrimental impact, one of which is cybercrime. Cybercrime is a crime that uses information technology. One of the smart phone technologies which includes cases of cybercrime that are often found in Indonesia include online prostitution of minors. This is done by utilizing social media, namely Michat as a medium of communication. The "chat with nearby users" feature by uploading a status that can be connected to the surrounding area within a certain radius and after being connected, the actor and his potential customer will negotiate and transact with each other until they finally meet. To eliminate digital evidence in the form of conversations in messages, usually perpetrators will delete the history of messages that produce data that can be used as evidence and perpetrators who can avoid legal traps, which are ultimately online. prostitution will be rampant. For online prostitution activities, it is necessary to carry out mobile forensics to find evidence which is then useful to be given to the authorities. This research uses the National Institute of Standards and Technology (NIST) method.

Keywords: *Cybercrime, Michat, Mobile Forensic, prostitusi online, Framework (NIST)*

1. PENDAHULUAN

Penggunaan smartphone semakin meningkat dari tahun ke tahun, menurut Statista penggunaan smartphone di Indonesia pada tahun 2019 mencapai 76,64 juta pengguna. Kelebihan smartphone antara lain untuk berinteraksi di media sosial dan melakukan video call. selain mempunyai kelebihan, smartphone juga memiliki dampak kerugian salah satunya adalah untuk melakukan cybercrime. Cybercrime adalah tindakan kejahatan yang memanfaatkan teknologi informasi. Salah satu penyalahgunaan smartphone yang termasuk kasus cybercrime yang cukup banyak ditemukan di Indonesia antara lain prostitusi online [1]. Didalam kasus prostitusi biasanya ada beberapa orang yang terlibat di dalam praktik prostitusi online diantaranya : mucikari, makelar, orang yang membantu memudahkan perbuatan cabul (pemilik kos / kontrakan yang dijadikan sebagai tempat dilakukannya prostitusi), dan PSK (pekerja seks komersial) itu sendiri. Dalam hal kejahatan prostitusi terhadap anak di bawah umur berdasarkan KUHP pasal yang relevan untuk menjerat orang-orang yang terlibat di dalamnya yaitu pasal 287 (1) dan (2), pasal 296, pasal 297 dan pasal 506 [2]. Terbongkarnya beberapa kasus prostitusi online yang diberitakan secara estafet oleh berbagai media di Indonesia, semuanya memiliki kesamaan dalam modus operasinya. Para pelaku memasarkan diri dan perempuan yang dijualnya melalui internet, baik dengan menggunakan website maupun jejaring sosial seperti MiChat, Facebook, Twitter, Blackberry Messenger, dan sebagainya.



Gambar 1. Persentase Medium Online

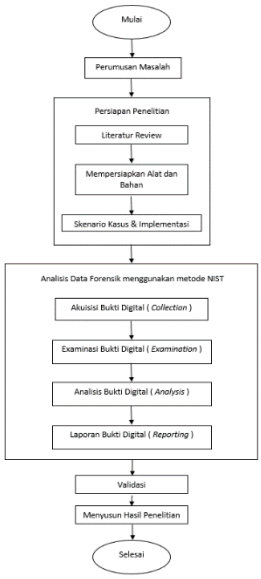
Berdasarkan data dari komisi Perlindungan Anak Indonesia (KPAI) mencatat terdapat 35 kasus eksploitasi seksual, perdagangan, dan pekerja anak terjadi selama Januari-April 2021. Dari jumlah tersebut, 60% di antaranya dilakukan melalui medium daring (online). Aplikasi MiChat yang merupakan aplikasi perpesanan instan gratis menjadi medium online yang paling banyak dipakai dalam kasus eksploitasi seksual, perdagangan, dan pekerja anak, yakni 41%. dan dalam kasus prostitusi online yang menggunakan aplikasi michat, ada kalanya untuk menghilangkan barang bukti kejahatan para pelaku terlebih dahulu menghapus barang bukti pada aplikasi tersebut seperti bukti chat percakapan transaksi, foto maupun video. dari data tersebut nantinya akan dikumpulkan dan dijadikan sebagai barang bukti digital forensic.

Maka dari itu dibutuhkan sebuah metode yang baik digunakan untuk melakukan analisis digital forensic pada aplikasi michat di smartphone. Metode National Institute of Standards Technology (NIST) adalah suatu standar atau pedoman untuk melakukan forensik pada perangkat mobile yang menjamin setiap examiner mengikuti alur kerja yang sama sehingga pekerjaan mereka terdokumentasikan dan hasilnya dapat di ulang serta dapat dipertahankan[3]. Metode ini juga banyak digunakan dalam hal penelitian sebelumnya seperti analisis forensik aplikasi telegram pada android menggunakan metode NIST [4], analisis forensik aplikasi beetalk menggunakan metode NIST [5] dan forensik mobile pada layanan media sosial LinkedIn menggunakan metode NIST [6]. Forensic digital merupakan cabang dari ilmu forensik yang mencakup penemuan selama investigasi data yang ditemukan pada perangkat digital sebagai barang bukti digital[7]. Mobile Forensic adalah ilmu untuk memulihkan bukti digital dari perangkat Mobile dibawah kondisi forensik menggunakan metode yang diterima. Mobile Forensic adalah cabang Digital Forensik [8].

Adapun tujuan yang akan dicapai dalam penelitian ini adalah mendapatkan bukti digital pada aplikasi MiChat untuk dijadikan bukti-bukti kejahatan sesuai dengan konsep forensic digital dan Mendapatkan hasil akuisisi pada tool – tool forensic yang digunakan dalam menganalisis MiChat sebagai salah satu proses dalam tahapan pembuktian digital.

2. METODE PENELITIAN

Alur penelitian ini dideskripsikan ke dalam bentuk flowchart. dengan adanya alur penelitian dapat membantu pelaksanaan penelitian lebih terstruktur dan sistematis.



Gambar 2. Alur metodologi penelitian

2.1. Persiapan Penelitian

Sebelum melakukan penelitian, dilakukan persiapan seperti literatur review dan mempersiapkan alat dan bahan untuk persiapan penelitian. Persiapan alat dan bahan antara lain adalah beberapa perangkat mobile android dan beberapa aplikasi untuk melakukan forensik terhadap perangkat mobile tersebut.

Tabel 1. Alat dan bahan

No	Nama Alat	Deskripsi	Keterangan
1	Laptop	Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz 2.60 GHz	*Hardware*
2	Windows 10	*Home Single Language*	Sistem Operasi
3	*Smartphone 1*	Xiaomi	*Hardware*
4	*Smartphone 2*	Samsung	Hardware
5	MobilEdit Forensik	Software Forensik	Tool Akuisisi
6	Wondershare Dr.Fone	Software Forensik	Tool Akuisisi

Penyusunan dan implementasi skenario dilakukan untuk merekontruksi aksi relevan yang mungkin dapat dilakukan oleh pelaku tindakan kriminal. Penyusunan skenario disusun berdasarkan analisis fungsionalitas dari perangkat mobile android dan referensi terkait. sebuah skenario kasus harus dijalankan untuk mendapatkan bukti digital. Pada penelitian ini peneliti membuat sebuah simulasi skenario lengkap dari aktivitas yang dilakukan pada aplikasi michat. Tujuan adanya skenario ini agar menjadi road map dari informasi yang diperlukan untuk di- recovery.

2.2. Analisis Digital Forensik Metode NIST

a. Akuisisi Bukti Digital, collection merupakan tahap paling awal dalam metode NIST[9], tahap ini adalah tindakan untuk pengamanan barang bukti. Tahap ini melakukan koleksi, identifikasi, rekaman atau pengambilan data dari sumber data yang relevan sesuai prosedur untuk menjaga integritas data.

b. Examinasi Bukti Digital (Examination), Tujuan dari proses *examination* ini adalah untuk mengambil serta menganalisis bukti digital yang ada. Ekstrak disini mengacu pada proses pemulihan data digital yang diperoleh atau *recovery* informasi dari suatu media forensik.

   Analisisnya mengacu pada metode yang telah ditetapkan dan menjadi standar forensik.

c. Analysis Bukti Digital (Analysis), Tahap Analysis merupakan tahap menganalisis atau tahap untuk melihat hasil dari tahap *Examination* yang sebelumnya secara detil untuk mendapatkan bukti digital pada barang bukti forensik. Hasil ekstraksi yang didapatkan dari proses *Examination* yang telah dilakukan pada dua *Smartphone* menggunakan tool MOBILedit Forensik dan Wondershare Dr.Fone mendapatkan hasil berupa data akun MiChat, nomor *handphone*, daftar kontak, pesan teks, gambar dan video.

d. Laporan Bukti Digital (Reporting**),** Tahap *Reporting* merupakan tahap pembuatan laporan berupa data-data hasil analisis pada tahap yang dilakukan sebelumnya, yang mencakup deskripsi bukti-bukti apa saja yang berhasil didapat dan presentasi keberhasilan alat forensik dalam melakukan ekstraksi dalam melakukan akuisisi barang bukti.

2.3. Validasi

Proses validasi diperlukan untuk menguji apakah hasil proses forensik yang diperoleh merupakan hasil yang benar, akurat, kredibel, dan menjaga *integritas* data sehingga dapat diakui di mata hukum. Hasil tes forensik setidaknya harus *repeatable* (dapat diulang kembali) dan *reproducible* (dapat diproduksi kembali) untuk menguji validitas hasil forensik dan dapat digunakan sebagai barang bukti [10]

2.4. Menyusun Hasil Penelitian

Pada tahapan ini merupakan tahap menyusun hasil analisis.yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai alat dan prosedur yang dipilih, penentuan tindakan lain yang perlu dilakukan, alat, dan aspek lain dari proses digital forensik. Serta pada tahapan ini peneliti juga memaparkan hasil akuisisi bukti digital pada tools forensik yang digunakan yakni *MobileEdit Forensic* dan *Wondershare Dr.Fone* dalam hal mendapatkan informasi barang bukti yang sudah dihilangkan oleh si pelaku. [11][3]

3. Hasil dan Pembahasan

3.1. Skenario Kasus

Pada penelitian ini dibuat skenario kasus seperti skema dibawah ini

Gambar 4. Skenario kasus

3.2. Identifikasi Barang Bukti Digital

Dalam proses identifikasi ditemukan beberapa solusi yang akan digunakan untuk membuktikan apakah barang bukti tersebut dapat digunakan didalam persidangan atau tidak. untuk melakukan hal tersebut maka peneliti dalam hal ini yang mana bertindak sebagai tim dalam bagian investigasi *forensic* digital akan melakukan akuisisi dan recovery data / mengembalikan data yang telah terhapus pada perangkat *mobile* tersebut.

3.3. Skenario sebelum dilakukan digital forensic

Sebelum melakukan digital forensik terdapat skenario yang dilakukan, smartphone Samsung sebagai pelaku A sedangkan *smartphone* Xiaomi Redmi Note 3 sebagai pelaku B antara lain:

1. Melakukan percakapan terkait kasus prostitusi online menggunakan media aplikasi *Michat*
2. Melakukan percakapan tranksasi pada *Michat*
3. Terdapat 23 data awal barang bukti digital yaitu 20 bukti digital gambar, 2 bukti digital video, dan 1 bukti digital audio
4. Percakapan yang telah dilakukan dan bukti digital yang terdapat pada *smartphone* telah dihapus semua sebelum melakukan digital forensik.

3.4 Digital Forensik Pada Bukti Digital Menggunakan Metode NIST Collection

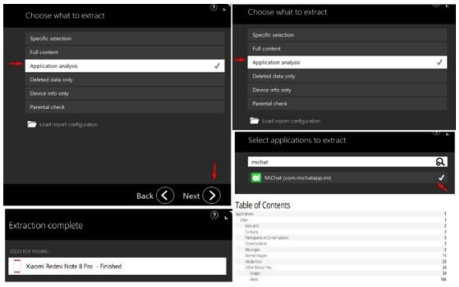
1. Collection

Gambar 5. Tahapan collection pada barang bukti

Analisis digital forensik pada tahap *Collection*, perlu dilakukan *isolation* terhadap kedua perangkat Smartphone dengan mengaktifkan *airplane mode* sehingga tidak ada jaringan yang aktif untuk menghindari modifikasi data. Proses *collection* juga akan mencatat spesifikasi dari barang bukti yang digunakan sebagai alat komunikasi pada transaksi prostitusi online anak dibawah umur

2. Examination

Proses ekstraksi data yang dilakukan yaitu smartphone yang menjadi barang bukti harus terlebih dahulu terkoneksi pada laptop tempat kedua tool forensik di-install.



Gambar 6. Proses ekstrasi pada Mobileedit

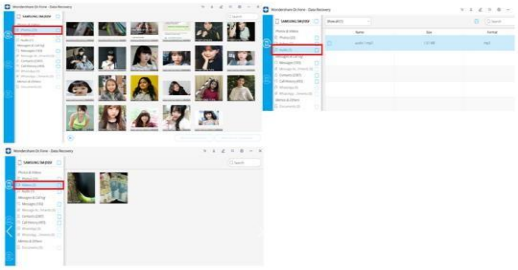
Gambar 7. Proses ekstraksi pada Wondershare

Hasil ekstraksi barang bukti oleh MobileEdit berhasil mengembalikan data terhapus berupa akun, kontak, chat, gambar, video, media files lainnya. berbeda ditunjukkan pada Wondershare yakni hasil ekstraksi pada barang bukti oleh Wondershare tidak dapat mengembalikan chat percakapan pada aplikasi michat dan hanya dapat mengembalikan data yang terhapus berupa gambar, video, dan data audio sementara akun dan chat tidak dapat dikembalikan.

3. Analisyt

Hasil analisis dari masing-masing tool ini dapat menjadi bukti bahwa data yang telah dihapus pada smartphone masih dapat di-recovery sehingga menjadi data pendukung pada penyelesaian suatu kasus kejahatan. Hasil examination data yang telah dihapus menggunakan tool Wondeshare hanya dapat mengembalikan data berupa gambar, video dan audio sementara data akun dan pesan chat pada aplikasi michat tidak dapat dikembalikan. Data terhapus yang berhasil dikembalikan oleh Wondershare pada barang bukti Jumlah data terhapus yang berhasil dikembalikan berupa gambar, video dan audio oleh

Wondershare pada barang bukti memiliki jumlah yang sama dengan data yang dihapus pada simulasi kasus yaitu 20 gambar, 2 video dan 1 audio. Data akun dan pesan chat aplikasi michat tidak memperoleh hasil apapun.



Gambar 8. Hasil Ekstrasi Barang bukti pada Wondershare

Gambar 9. Hasil Ekstrasi Barang bukti pada MobileEdit

Berdasarkan gambar diatas jumlah data terhapus yang berhasil dikembalikan berupa akun, data kontak, chat, gambar, video, dan audio oleh MobileEdit pada barang bukti memiliki jumlah yang sama dengan data yang dihapus pada simulasi kasus yaitu sebanyak 2 data kontak, chat pada aplikasi michat, 20 gambar, dan 2 video. Data berbeda ditunjukkan oleh data pesan yang berhasil dikembalikan yaitu sebanyak 15 chat dari 15 data yang dihapus pada simulasi kasus. Hasil analisis menunjukkan bahwa data chat yang dihapus dapat kembali ditemukan oleh tool MobileEdit. Berbeda dengan hasil recovery pada data audio terhapus yang tidak dapat dikembalikan oleh MobileEdit, hasil recovery data audio tidak memberikan hasil yang diharapkan karena data yang telah dihapus pada barang bukti tidak dapat dikembalikan.

4. Reporting

Dapat diketahui bahwa pada laporan digital forensik terkait barang buktismartphone yang dianalisis bahwa penerimaan bukti diterima tanggal 19 Juni 2021. Deskriptif kasus adalah menemukan dan memulihkan data yang diajukan. Data yang diajukan adalah akun, data kontak, gambar video, audio, dan pesan chat. Peralatan yang digunakan selama proses digital forensik adalah aplikasi MobileEdit dan Wonderhare dr.fone serta USB Cable. Detail temuan yang ditemukan adalah terdapat gambar,video,audio serta pesan chat yang terindikasi dihapus atau disembunyikan.

Hasil Kinerja Tools Forensic dalam proses akuisisi bukti digital

Hasil analisis forensik yang dilakukan dari 6 jenis data yang menjadi fokus pengembalian data (akun, data kontak, gambar, video, audio, dan pesan chat), MobileEdit berhasil mengembalikan 5 jenis data yang telah dihapus, sedangkan Wondershare berhasil mengembalikan 3 jenis data yang telah dihapus. Berikut adalah tabel hasil pengujian dari 2 tool forensik pada barang bukti smartphone.

Tabel 2. Hasil Akuisisi Bukti digital pada MobileEdit

Sumber Bukti Digital	Digital Forensik Menggunakan Aplikasi MobileEdit			
	Xiaomi Redmi Note 8		Samsung Galaxy J1 mini	
	Data Awal	Data Setelah	Data Awal	Data Setelah
Sumber Bukti Digital				
Akun	1	1	1	1
Data kontak	2	2	2	2
Gambar	20	20	20	20
Video	2	2	2	2
Audio	1	0	1	0
Pesan Chat	15	15	15	15

Tabel 3. Hasil Akuisisi Bukti digital pada Wondershare

Sumber Bukti Digital	Digital Forensik Menggunakan Aplikasi Wondershare			
	Xiaomi Redmi Note 8		Samsung Galaxy J1 mini	
	Data Awal	Data Setelah	Data Awal	Data Setelah
Sumber Bukti Digital				
Akun	1	0	1	0
Data kontak	2	0	2	0
Gambar	20	20	20	20
Video	2	2	2	2
Audio	1	1	1	1
Pesan Chat	15	0	15	0

Keterangan:
Data Awal: Data yang telah dipersiapkan sebelum dihapus.
Data Setelah: Data yang telah dihapus dan ditemukan atau dipulihkan

Dari tabel diatas didapatkan perbandingan hasil kinerja tools forensic dari smartphone menggunakan MobileEdit Forensic dan Wondershare Dr.Fone adalah MobileEdit Forensic berhasil mendapatkan data bukti gital mencapai 5 jenis data dari 6 data yang disimulasikan dalam mengembalikan data terhapus dengan jumlah total data yakni 40 data, sedangkan dengan wondershare dr.fone hanya berhasil mendapatkan data bukti gital mencapai 3 jenis data dari 6 data yang disimulasikan dengan total 23 data.

Berdasarkan hasil akuisisi bukti digital yang diperoleh menggunakan 2 tool forensik MobileEdit Forensic dan Wondershare Dr.Fone pada 2 smartphone yang menjadi barang bukti maka dapat diketahui bahwa hasil recovery data yang telah dihapus dengan tool MobileEdit Forensic lebih signifikan dibandingkan dengan Wondershare Dr.Fone.

4. Kesimpulan

Pada akuisisi bukti digital smartphone berhasil mengembalikan data yang sudah terhapus dengan hasil kinerja pada tools MobileEdit Forensic pada barang bukti smartphone menggunakan NIST dari 6 jenis data yang telah dipersiapkan pada simulasi, Mobileedit dapat mengembalikan atau memulihkan 40 data dari 41 data yang dipersiapkan. Pada perbandingan bukti digital menggunakan aplikasi wondershare Dr.Fone hanya dapat mengembalikan atau memulihkan 23 data dari 41 data yang telah dipersiapkan. Dan Dengan data hasil recovery bukti digital dengan tool MobileEdit sangat direkomendasikan sebagai barang bukti dalam membuktikan kasus kejahatan dalam persidangan. Untuk pengembangan pada penelitian berikutnya dapat ditambahkan dengan smartphone dan sistem operasi yang berbeda sehingga hasil yang diperoleh menjadi tolak ukur yang baik dari perbandingan performa kinerja kedua tool yang digunakan.

DAFTAR PUSTAKA

[1] I. Riadi, S. Sunardi, and M. E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *J. Tek. Elektro*, vol. 10, no. 1, pp. 18–22, 2018, doi: 10.15294/jte.v10i1.14070.

[2] M. N. Rizky, R. I. Fitriani, M. W. Sudibyo, F. A Husnasari, and F. Maulana, "Perlindungan Hukum Terhadap Anak Korban Eksploitasi Seksual Komersial Melalui Media Sosial," *Media Iuris*, vol. 2, no. 2, p. 197, 2019, doi: 10.20473/mi.v2i2.13193.

[3] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[4] I. G. N. Guna Wicaksana and I. K. Gede Suhartana, "Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 8, no. 4, p. 381, 2020, doi: 10.24843/jlk.2020.v08.i04.p03.

[5] M. I. Syahib, I. Riadi, and R. Umar, "Analisis Forensik Digital Aplikasi Beetalk untuk Penanganan Cybercrime Menggunakan Metode NIST," *Semin. Nas. Inform.*, vol. 2018, no. November, p. 134, 2018, [Online]. Available: http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/26_29.

[6] I. Riadi, A. Yudhana, and M. Al Barra, "Forensik Mobile pada Layanan Media Sosial LinkedIn," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 6, no. 1, pp. 9–20, 2021, doi: 10.14421/jiska.2021.61-02.

[7] S. RACHMIE, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," *Litigasi*, vol. 21, no. 21, pp. 104–127, 2020, doi: 10.23969/litigasi.v21i1.2388.

[8] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, "Mobile Forensics: Advances, Challenges, and Research Opportunities," *IEEE Secur. Priv.*, vol. 15, no. 6, pp. 42– 51, 2017, doi: 10.1109/MSP.2017.4251107.

[9] M. Fitriana, K. A. AR, and J. M. Marsya, "Penerapana Metode National Institute of Standars and Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, p. 29, 2020, doi: 10.22373/cj.v4i1.7241.

[10] V. G. Larenda, M. Unik, and H. Mukhtar, "Analisis SMS Forensik Smartphone sebagai Rujukan Menghadirkan Barang Bukti yang Sah di Pengadilan," 2016.

[11] S. Azizah, S. A. Ramadhona, and K. W. Gustitio, "Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST," *J. Repos.*, vol. 2, no. 10, pp. 1400-1405, 2020, doi: 10.22219/repositor.v2i10.1066.

[12] Soni, Prayudi, Y., & Sugiantoro, B. (2017). Teknik Akuisisi Virtualisasi Server Menggunakan Metode Live Forensic. Teknomatika, 9(2).

[13] S, S., Hafid, A., & Sudyana, D. (2019). Analysis of Security Awareness in using Technology and Social Media at Muhammadiyah University of Riau. International Journal of Computer Applications, 177(18), 20–25. https://doi.org/10.5120/ijca2019919631

[14] Soni, Prayudi, Y., Sugiantoro, B., Sudyana, D., & Mukhtar, H. (2019). Server Virtualization Acquisition Using Live Forensics Method. 190, 18–23. https://doi.org/10.2991/iccelst-st-19.2019.4

[15] Sudyana, D., Putra, R. T., & Soni, S. (2019). Digital Forensics Investigation on Proxmox Server Virtualization Using SNI 27037:2014. Sinkron, 3(2), 67–72. https://doi.org/10.33395/sinkron.v3i2.10029.

[16] Soni, S., Fatma, Y., & Anwar, R. (2022). Akuisisi Bukti Digital Aplikasi Pesan Instan "Bip"Menggunakan Metode National Institute Of Justice (NIJ). Jurnal CoSciTech (Computer Science and Information Technology), 3(1), 34–42. https://doi.org/10.37859/coscitech.v3i1.3694